receive a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network, such that said hosts inherit said definitions associated with an assigned role;

receive an assignment of roles to said hosts in said network; and

generate said security policy from said received definitions and assignments.

REMARKS

This Amendment is submitted in response to the outstanding final Office Action, dated September 5, 2002. Claims 1 through 8, 29 through 35 and 38 are presently pending in the above-identified patent application. Claims 9-28, 36 and 37 were withdrawn from consideration, without prejudice, in a prior response. Claims 1, 29, 35 and 38 have been amended. No additional fee is due.

The Examiner is thanked for a brief telephone interview on November 20, 2002 in which the Arrow reference was discussed. The "inheritance" aspect of the invention was also discussed, but no agreement was reached on patentability.

This amendment is submitted pursuant to 37 CFR §1.116 and should be entered. The Amendment places all of the pending claims, i.e., claims 1 through 8, 29 through 35 and 38, in a form that is believed allowable, and, in any event, in a better form for appeal. It is believed that examination of the pending claims as amended, which are consistent with the previous record herein, will not place any substantial burden on the Examiner. In addition, this Amendment is being presented following a productive telephone interview with the Examiner in an attempt to reach an agreement on patentable subject matter. Applicants submit that this Amendment could not have been proposed any sooner.

In the final Office Action, the Examiner rejected Claim 29 under 35 U.S.C. §103(a) as being unpatentable over Reid et al. (United States Patent Number 6,182,226) in view of Arrow et al. (United States Patent Number 6,175,917). In addition, the Examiner rejected Claims 1-8, 29-35 and 38 under 35 U.S.C. §103(a) as being unpatentable over Reid et al. in view of Grennan, "Firewalling and Proxy Server HOWTO," Nov. 1996, and further in view of Arrow et al.

The present invention is directed to a firewall manager that generates a security policy for a particular network environment, and automatically generates the firewall-specific configuration files from the security policy simultaneously for multiple gateways. The security policy is expressed in terms of "roles," which are used to define network capabilities of sending and receiving services. Roles capture the topology-independent and firewall-independent essence of a policy. A role is a property

that may be assumed by different hosts in the network. If a host is assigned as a role, the host will *inherit* the firewall properties of the role.

The Examiner rejected Claim 29 under 35 U.S.C. §103(a) as being unpatentable over Reid et al. in view of Arrow et al. The Examiner asserts that Reid et al. discloses restricting the communication of packets to and from network interfaces using a set of policies (rules) configured corresponding to the region (assignment of roles) that the network interface is assigned. The Examiner further asserts that the firewall comprises a plurality of regions (assignment of roles) having policies (rules) configured (generated) for each of the regions. Citing col. 2, lines 8-17. The Examiner notes that Reid et al. disclose various commands for setting up access control rules that are applied to the regions (assignment of roles) in column 11.

The Examiner acknowledges that Reid et al. do not disclose or suggest that roles may be assigned to hosts independently of a topology of a network. The Examiner asserts, however, that Arrow et al. disclose an access control role (policy) that specifies that communications between non-members (independent hosts of the topology) of a VPN and members of a VPN are not allowed to pass through a particular VPN unit (citing col. 15, lines 63-67).

In Arrow, access control rules specify which types of communications can pass through a VPN unit. Col. 15, lines 61-62. "For example, an access control rule can specify that communications between non-members of a VPN and members of a particular VPN are not allowed to pass through a particular VPN unit." Id. The "members" are merely the machines of a virtual private network (VPN) each identified by a fixed IP address and are physically connected to the VPN. A firewall on the VPN provides physical separation between the members and non-members. Each IP address may have an associated label ("X"), and the access control rules specify whether to allow or deny particular communications to the machine X. Thus, "members" and "non-members" of Arrow et al. are thus clearly network-topology dependent and the ability of a machine to send and receive packets cannot be "assigned to said machines independently of a topology of said network," as required by each of the independent claims.

Furthermore, each of the claims have been amended to emphasize that host machines inherit the firewall properties of an assigned role. Thus, Arrow does not disclose or suggest that "said hosts inherit said definitions associated with an assigned role," as required by each of the independent claims, as amended.

The Examiner also rejected Claims 1-8, 19-28, 30-35 and 38 under 35 U.S.C. §103(a) as

being unpatentable over Reid et al. in view of Grennan and further in view of Arrow et al. Grennan was cited by the Examiner for its teaching of the generation of a configuration file for a firewall. (citing section 4.2). Grennan discloses the generation of a configuration file for a *specific* firewall. In any case, Grennan does not disclose or suggest "receiving a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network, such that said hosts inherit said definitions associated with an assigned role," as required by each of the independent claims, as amended. Support for the amendments are found, for example, at pages 7-8. Applicants submit that it was not known to use inheritance principles in the context of a firewall system.

Claims 2 through 8 and 30 through 34 are dependent on Claims 1 or 29 and are therefore patentably distinguished over Reid et al., Grennan or Arrow, alone or in combination, because of their dependency from independent Claims 1 or 29 for the reasons set forth above, as well as other elements these claims adds in combination to their base claim. For example, claim 3 specifies that a security policy for said network is "expressed in terms of said roles defining network capabilities of sending and receiving services." Claims 4 and 32 specify that a plurality of roles are "combined into role-groups that may be assigned to one or more hosts." Claims 5 and 33 specify that a plurality of hosts are "combined into a host-group that may be assigned a role or a role-group." Reid et al., Grennan or Arrow, alone or in combination, do not disclose or suggest the idea of "roles," as used in the present invention.

In view of the foregoing, the invention, as claimed in Claims 1 through 8, 29 through 35 and 38 cannot be said to be either taught or suggested by Reid et al., Grennan or Arrow, alone or in combination. Accordingly, applicants respectfully request that the rejection of claim 1 through 8, 29 through 35 and 38 under 35 U.S.C. § 103 be withdrawn.

All of the pending claims, i.e., claims 1 through 8, 29 through 35 and 38, are in condition for allowance and such favorable action is earnestly solicited.

If any outstanding issues remain, or if the Examiner has any further suggestions for expediting allowance of this application, the Examiner is invited to contact the undersigned at the telephone number indicated below.

The Examiner's attention to this matter is appreciated.

Respectfully,

Kevin M. Mason

Date: November 21, 2002

Kevin M. Mason
Attorney for Applicant(s)
Reg. No. 36,597
Ryan, Mason & Lewis, LLP
1300 Post Road, Suite 205
Fairfield, CT 06430
(203) 255-6560

VERSION MARKED TO SHOW ALL CHANGES

IN THE CLAIMS:

Please amend the claims as follows:

1. (Twice Amended) A method for generating a configuration file for at least one firewall in a network, said network including a plurality of hosts, said method comprising the steps of:

receiving a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network, such that said hosts inherit said definitions associated with an assigned role;

receiving an assignment of said roles to said hosts in said network; and

generating rules for said hosts based on said assigned roles, said rules determining whether a packet is passed to a destination host.

29. (Twice Amended) A method of generating a security policy for a network, said network including a plurality of hosts, said method comprising the steps of:

receiving a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network, such that said hosts inherit said definitions associated with an assigned role;

receiving an assignment of said roles to said hosts in said network; and

generating said security policy from said received definitions and assignments.

35. (Twice Amended) A compiler for generating a configuration file for a firewall in a network, said network including a plurality of hosts, comprising:

a memory for storing computer-readable code; and

a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to:

receive a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network, such that said hosts inherit said definitions associated with an assigned role;

receive an assignment of said roles to said hosts in said network; and

generate rules for said hosts based on said assigned roles, said rules determining whether a packet is passed to a destination host.

38. (Twice Amended) A system for generating a security policy for a network, said network including a plurality of hosts, said system comprising:

a memory for storing computer-readable code; and

a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to:

receive a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network, such that said hosts inherit said definitions associated with an assigned role;

receive an assignment of roles to said hosts in said network; and

generate said security policy from said received definitions and assignments.